Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

THE

AMERICAN

MATHEMATICAL MONTHLY

VOLUME XX MAY, 1913 NUMBER 5

THE FOUNDATION PERIOD IN THE HISTORY OF GROUP THEORY.

By JOSEPHINE E. BURNS, University of Illinois.

The Earliest Group Notions.—Henri Poincaré has pointed out that the fundamental conception of a group is evident in Euclid's work; in fact that the foundation of Euclid's demonstrations is the group idea. Poincaré establishes this assertion by showing that such operations as successive superposition and rotation about a fixed axis presuppose the displacements of a group. However much the fundamental group notions were unconsciously used in the work of early mathematicians, it was not until the latter part of the eighteenth century that these notions began to take life and develop.

The Foundation Period.—The period of foundation of group theory as a distinct science extends from Lagrange (1770) to Cauchy (1844–1846), a period of seventy-five years. We find Lagrange considering the number of values a rational function can assume when the variables are permuted in every possible way. With this beginning the development may be traced down through the contributions of Vandermonde, Ruffini, Abbati, Abel, Galois, Bertrand and Hermite, to Cauchy's period of active production (1844–1846). At the beginning of this period group theory was a discovery useful in the theory of equations; at the end it existed as a distinct science, not yet, to be sure, entirely free but so nearly so that this may be called the close of the foundation period.

LAGRANGE, RUFFINI, GALOIS.

Lagrange.—The contributions of Lagrange are included in his memoir, *Reflexions sur la résolution algébrique des equations,* published in the Mémoirès of the Academy of Science at Berlin in 1770–1771.[1] In this paper Lagrange first applies what he calls the "calcul des combinaisons" to the solution of algebraic equations. This is practically the theory of substitutions, and he uses it to show wherein the efforts of his predecessors, Cardan, Ferrari, Descartes, Tschirnhaus, Euler and Bezout fail in the case of equations of degree higher than the fourth. He studies the number of values a rational function can assume when its variables are permuted in every possible way. The theorem that the order of the subgroup divides the order of the group is implied but not explicitly proved. The theorem that the order of a group of degree n divides $n!$ is however explicitly stated. Lagrange does not use at all the notation or the terminology of group theory but confines himself entirely to direct applications to the theory of equations. He mentions the symmetric group of degree 4, and the four-group and the cyclic group of order 4 as subgroups of this group. This embodies practically all of the work of Lagrange in the theory of substitution groups.

---

[1] *Œuvres de Lagrange,* vol. 3, pp. 204–420.

Ruffini.—The first man to follow Lagrange and to make any signal progress was Paolo Ruffini, an Italian, who published in 1799 in his *Teoria generale della equazioni* a number of important theorems in the theory of substitutions. Burkhardt says[1] that several fundamental concepts are implied, if not explicitly stated. Ruffini's "permutation" corresponds to the later accepted term of group and to Cauchy's "system of conjugate substitutions." These permutations he classifies as "simple" and "complex." The first are of two sorts, of one cycle or of more than one cycle. The second he divides into three classes which correspond to the modern notions of (1) intransitive, (2) transitive imprimitive, and (3) transitive primitive. He enunciates the following theorems:

1. If a substitution of n letters leaves the value of a rational function invariant, the result of applying the substitution any number of times is that the function is left invariant.
2. The order of a substitution is the least common multiple of the orders of the cycles.
3. There is not necessarily a subgroup corresponding to every arbitrary divisor of the order of the group.

This theorem he established by showing that there is no eight-valued, four-valued or three-valued function on five letters.

4. A group of degree five that contains no cycle of degree five cannot have its order divisible by five.

Abbati, Abel.—From Ruffini to Galois, only two or three contributions of merit were made. Abbati gave the first complete proof that the order of the subgroup divides the order of the group. This he did by putting the substitutions of the group in rectangular array. Abbati also proved that there is no three or four valued function on n letters when n is greater than five. Cauchy published in 1815 a relatively unimportant memoir. Abel, by using the theory of substitutions to prove that it is impossible to solve algebraically equations of degree higher than the fourth, called attention to this useful instrument.

Galois.—Up to the time of Cauchy, Galois had done the most for group theory. His work was written in 1831 and 1832, but not made public until 1846. To Galois is due the credit for the conception of the invariant subgroup, for the notion of the simple group and the extension of the idea of primitivity. Galois first used the term group in its present technical sense. Several important theorems are due to him. Among these are the following:

1. The lowest possible composite order of a simple group is 60.[2]
2. The substitutions common to two groups form a group.[3]

---

[1] *Zeitschrift für Math. u. Phys.* (1892), 37, p. 119.

[2] *Œuvres Mathématiques d' Éveriste Galois*, p. 26.

[3] *Manuscrits de Éveriste Galois*, p. 39.

3. If the order of a group is divisible by p, a prime, there is at least one substitution of order p.
4. The substitutions of a group that omit a given letter form a group.

CAUCHY, THE FOUNDER OF GROUP THEORY.

Terminology.—Cauchy's work on groups is found in his *Exercises d'analyse et de physique mathematique* published in 1844, and in the series of articles published in the Paris *Comptes Rendus* in 1845–1846.[1] Cauchy defines permutation and substitution in the same way, but uses the latter term almost entirely. He uses several devices to denote a substitution, the most common being (x, y, z, u, v, w) where each letter is replaced by the one which follows it and the last by the first. He defines this as a cyclic substitution. In the article written in 1815[2] he defines the degree of a substitution as the first power of the substitution that reduces to identity, but later he also defines order in this way and uses the word order rather than degree in his subsequent work. He uses both the term unity and identical substitution. A transposition is defined and the terms similar, regular, inverse and permutable substitutions are found with their present day significance. A group he calls a "system of conjugate substitutions," which may be transitive or intransitive. A transitive imprimitive group is "transitive complex." The order of a system of conjugate substitutions is the number of substitutions that it contains. The term "divisor indicatif" is also found for the order of a group. Cauchy frequently transfers his definition of order to the theory of equations and speaks of the number of equal values a rational function can assume when the variables are permuted in every possible way. The number of distinct values of such a function is the index. In the early article the order of operation is from left to right, but in all his later work he reverses the order and operates from right to left.

The Memoir of 1815.—In the paper published in 1815 the one theorem which is of special interest is that the number of distinct values of a non-symmetric function of degree n cannot be less than the largest prime that divides n, without becoming equal to 2. This theorem is proved. He states the special cases, that if the degree of a function is a prime number greater than 2, the number of distinct values cannot be less than the degree; and that if the degree is 6 the number of distinct values cannot be less than 6. He makes special reference to the functions belonging to (1) the intransitive group of degree 6 and order 36; (2) the transitive imprimitive group of degree 6 and order 72; (3) the intransitive group of degree 6 and order 48; (4) and the symmetric group of degree 5 considered as an intransitive group of degree 6. The functions are as follows:

$$(1)\quad a_1a_2a_3 + 2a_4a_5a_6, \qquad (3)\quad a_1a_2a_3a_4 + a_5a_6,$$

$$(2)\quad a_1a_2a_3 + a_4a_5a_6, \qquad (4)\quad a_1a_2a_3a_4a_5 + a_6.$$

The Memoir of 1844.—In the memoir published in 1844 in his *Exercices d'Analyse* there is much more of importance. The first theorem proved is that every substitution similar to a given substitution P is the product of three factors, the extremes of which are the inverse of each other and the middle term of which is P. Conversely, every product of three factors, the first and last of which are the inverse of each other, is similar to the middle term P. An important formula developed is for the number of substitutions similar to a given substitution. If ω is the number required, n the total number of letters and P the given substitution, composed of f cycles of order a, g cycles of order b, h cycles of order c, etc., and r the number of letters fixed in P, then

---

[1] *Œuvres de A. Cauchy,* First series, vols. 9 and 10.

[2] *Journal de l'Ecole polytechnique,* 10 (1815), p. 1.

$$\omega = \frac{n!}{(f!)(g!)(h!)\cdots(r!)a^f b^g c^h \cdots}.$$

Among other theorems that he proves in this article are the following:

1. If P is a substitution of order i, h any number and θ the highest common factor of h and i, then P^h is of order i/θ.
2. If P is a substitution of order i, the substitutions among the powers of P that are of order i are the powers of P whose indices are prime to i. These substitutions are likewise similar to P, and hence the number of substitutions similar to P among the powers of P are in number equal to the number of numbers less than i and prime to it.
3. Let P be any substitution, regular or irregular; let i be its order and p any prime factor of i. Then a value for i can always be found such that P^i is a substitution of order p.
4. A substitution and its inverse are always similar.
5. The powers of a cycle constitute the totality of substitutions that transform the given cycle into itself.
6. The order of a system of conjugate substitutions is divisible by the order of each substitution.
7. Two permutable substitutions with no common power but identity, together generate a system of conjugate substitutions whose order is the product of the orders of the two substitutions.
8. If $1, P_1, P_2, \cdots P_{a-1}$ and $1, Q_1, Q_2, \cdots Q_{b-1}$ are two groups, one of order a and the other of order b, which are permutable and have no common terms but identity, then the group generated by these groups is of order ab.
9. The converse of (8).
10. If P and Q are two substitutions, one of order a and the other of order b, and if the two series $Q, PQ, P^2Q, \cdots P^{a-1}Q$ and $Q, QP, QP^2, \cdots QP^{a-1}$ are made up of the same terms in the same or different order, then the cyclic group generated by P is permutable with the cyclic group generated by Q.

A most important element in establishing Cauchy's claim as the founder of group theory is the proof which he gives of the fundamental theorem that if m is the order of a group and p any prime which divides m, there is at least one substitution of order p. Galois had stated the theorem but had not proved it. Its importance is due to the fact that it is the first step toward Sylow's theorem which appeared nearly thirty years later. In this memoir there are a number of specific groups mentioned although no enumeration of groups of special degrees is attempted. The substitutions of several groups are written out. Among them are (1) the octic, (2) the four-group, (3) the holomorph of the cyclic group of order five, (4) the intransitive group of degree 6 and order 9 and (5) the intransitive group of degree 6 and order 16. In addition to these groups the substitutions of which are given, several other groups are mentioned, among them (1) the holomorph of order 42, (2) the group of degree 7 and order 21, (3) the holomorph of the cyclic group of order 9.

There is also mentioned a group of degree 9 and order 27, generated by the two substitutions

$$P \equiv x_0x_3x_6 \cdot x_1x_4x_7 \cdot x_2x_5x_8 \quad \text{and} \quad Q \equiv x_1x_2x_4x_8x_5 \cdot x_3x_6.$$

This is obviously impossible but a little study of his method reveals that he should have used $Q \equiv x_1x_3x_4x_8x_7x_5 \cdot x_3x_6$, and that in order to get the order of the group he has incorrectly applied the theorems he was announcing and illustrating. The order of the group should be 18. The two theorems which he was illustrating may be stated as follows:

1. If P is a substitution on n letters, $P = x_0x_1x_2 \cdots x_{n-1}$, and if r is any number prime to n and if Q is a substitution derived from P by replacing each letter by another whose subscript is r times its own, then for any values of h and k

$$Q^kP^h = P^{r^kh}Q^k.$$

2. If in the above theorem we take v any divisor of n, distinct from unity, and let R be any substitution that replaces any letter x_l by the letter with the subscript $l + v$, then Q^kR^h generates a group of order vi, where i is the smallest value of k that satisfies the congruence $r^k \equiv i \pmod{n}$.

Since in the present instance r is 2, i must be 6. The order of the group is then $vi = 3 \cdot 6 = 18$, whereas Cauchy seems to take $i = 9$ and derives the order of the group $vi = 3 \cdot 9 = 27$.

The Memoirs of 1845–1846.—Some of the material in the memoirs[1] published in the *Comptes Rendus* had already appeared in the *Exercices*, but is treated more extensively here. There is much, however, in the later articles that is not touched in the *Exercices*. It is in the later memoirs that he first defines what he means by a system of conjugate substitutions. The definition is as follows:

> I shall call derived substitutions all that can arise from the given substitutions by multiplying them one or more times by each other or by themselves; and the given substitutions together with all the derived substitutions form what I shall call a system of conjugate substitutions.

Then follow the general theorems:

1. If i is the order of a substitution P and $a, b, c, \cdots$ are the prime factors of i, then the substitution P and its powers form a group generated by the substitutions $P^{i/a}, P^{i/b}, P^{i/c} \cdots$.
2. If $P, Q, R, S, \cdots$ are the substitutions that leave a given function Ω invariant, they form a group whose order is the number of equal values of Ω when the variables are permuted in every possible way.
3. The order of a transitive group of degree n is n times the order of the subgroup that leaves one letter fixed.
4. If Ω is a transitive function on n letters, if m is the index of the corresponding transitive group under the symmetric group of degree n, then m will likewise be the index of the subgroup that leaves one letter fixed under the symmetric group of degree $n - 1$.

Intransitive Groups.—The general subject which Cauchy treats next is that of intransitive groups. He implicitly divides intransitive groups into two classes. The first class includes those in which the systems are independent, that is, in our terminology, those in which the systems of transitivity are united by direct product. The second class includes those in which the systems are dependent, that is, those in which the systems are united by some sort of isomorphism. The concept of isomorphism is however only implied. He states first that an intransitive group is formed by the combination in some way of transitive constituents. He then develops some interesting formulas for the order of intransitive groups. If the systems are independent, then the order M is the direct product of $A, B, C, \cdots$ the orders of the transitive constituents and the index will be $n!/ABC \cdots$ where n is the total number of letters. This same formula holds also when the systems are not independent if $A, B, C \cdots$ are defined in a special way. These definitions are as follows:

---

[1] *Œuvres de A. Cauchy*, First series, volumes 9 and 10.

> Let A be the order of the first transitive constituent;
>
> Let B be the number of substitutions involving letters in the second system without involving any of the first;
>
> Let C be the number of substitutions involving letters in the third system, without involving any of the first or second, and so on.

With these definitions of $A, B, C, D \cdots$ the order of the intransitive group is $M = ABC \cdots$.

Imprimitive Groups.—Cauchy next turns to imprimitive groups. Here he confines himself almost entirely to the consideration of those imprimitive groups which are simply transitive and which have for the subgroup that leaves one letter fixed the direct product of the transitive constituents. In regard to this particular type of imprimitive groups, he gives several theorems which are of interest, even though he does not touch upon the broader and more general principles.

If in a simply transitive group the subgroup that leaves one letter fixed is an intransitive group formed by the direct product of its transitive constituents, the group is imprimitive. He considers the special cases $a > n/2$, $a < n/2$, $a = n/2$ in which a, the number of letters in the largest transitive constituent and n is the degree of the group.

The only theorems which he enunciates that apply to imprimitive groups in general are:

> 1. The number of letters in the systems of imprimitivity must be a divisor of the degree.
> 2. If A is the number of substitutions that permute the variables within the systems and K the number of ways the k systems can be permuted, then the order of the group is KA^k.

Symmetric Groups.—Cauchy then considers briefly symmetric groups. One theorem which he states with its corollaries is as follows:

> If a transitive group of degree n has a symmetric subgroup of degree a, where $a > n/2$, then the group is symmetric on n letters.
>
> For $n > 2$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 1$.
>
> If $n > 3$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 2$. The special case $n = 4$ is excepted; for the octic group, belonging to the function $\Omega = xy + zu$ is symmetric on two letters, yet not symmetric on all four.
>
> If $n > 4$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 3$. The case $n = 6$ is excluded. A group requiring this exception is the imprimitive group of degree 6 and order 72 which contains the symmetric group of order 6.
>
> If $n > 5$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 4$. If $n = 6$ or $n = 8$, this does not hold. Cauchy gives as examples of the case $n = 6$ the imprimitive groups of degree 6 and orders 72 and 48.

Some Implied Theorems.—One of the most important and interesting parts of Cauchy's work on group theory is that in which he develops some complicated formulas from which we may easily deduce the theorem that the average number of letters in the substitutions of a transitive group is $n - 1$. Cauchy himself does not enunciate the theorem, although he brings the proof to the point where only the final statement is necessary to complete it. The formula for the case where the group is simply transitive is as follows:

$M = 2H_{n-2} + 3H_{n-3} + \cdots + (n-2)H_2 + n$ where M is the order of the group, n its degree and H_{n-r} the number of substitution involving $n - r$ letters.

Further development of these formulas leads to the two conclusions:

1. If G is l-fold transitive of degree n, the number of substitutions involving $n - l + 1$ letters is equal to or greater than $n(n-1) \cdots (n-l+2)/(n-l)\, l!$;
2. If G is simply transitive, of degree n, the number of substitutions involving n letters is equal to or greater than $n - 1$.

We find here the assertion that if in an l-fold transitive group $l + 1$ letters are left fixed, all are left fixed. That this is false is demonstrated by considering the imprimitive group of degree 6 and order 72. It is simply transitive and hence $l = 1$; but $l + 1 = 2$ letters may be left fixed without all being so.

The theorem that the order of the holomorph of a cyclic group is the product of the orders of the cyclic group and its group of isomorphisms is found implicitly in Cauchy. He gives two theorems relative to this point.

1. Let $P = x_0x_1x_2 \cdots x_{n-1}$ be a substitution of order n. Let r be a primitive root of the modulus n, and I the smallest of the indices of unity belonging to the base r. Then let Q be the substitution that replaces x_l by x_{rl}. The order of Q will be I and the order of the group will be nI.

   This I is nothing else than the order of the group of isomorphisms of the cyclic group. If n is a power of a prime p, then $I = n(1 - 1/p)$. When n is a prime then $I = n - 1$.
2. With the same hypothesis as in (1), P^a and Q^b, where a and b are divisors of n and I respectively, generate a group of order nI/ab.

Enumeration of Orders.—Cauchy was the first to attempt an enumeration of the possible orders of groups. This he did with a fair degree of accuracy up to and including the sixth degree. The enumeration including degree 5 is correct and complete, but several errors occur in the enumeration of those of degree 6. For instance, 150 is given as the index of a group of degree 6 under the symmetric group, although factorial six is not a multiple of 150.

Cauchy goes back to his original distinction between imprimitive groups with heads which are direct products and those with heads formed by isomorphisms. He gives as the possible orders of groups of degree 6 with heads the direct products of the transitive constituents, 72, 48, 24, 18, 16, and 8. The last two numbers are clearly impossible for there is no transitive group of degree 6 and order 8 or 16. The orders of the groups possible when the head is formed with isomorphisms are given as 6, 12, 4, while there is no imprimitive group of degree 6 and order 4. According to his classification there should also be included in this last enumeration 24 and 18. A complete omission occurs in the list of imprimitive groups since the groups of order 36 with two systems of imprimitivity are not mentioned. Otherwise the enumeration through degree 6 is correct and complete.

Errors of Cauchy.—The errors in Cauchy's work on group theory may be divided into two classes. The first and smaller class includes a number of serious errors in logic. The second class includes a large number of minor errors, some typographical, others arising through careless statement. All of the serious errors found have been noted in this paper with the exception of one to which attention has already been called.[1] He states an erroneous theorem on imprimitive groups in the following form.

> If G_1 is a subgroup composed of all the substitutions that omit a given letter in a simply transitive group then G is imprimitive unless all the transitive constituents of G_1 are of the same degree.

Conclusion.—In conclusion we may say that the foundation period in the history of group theory includes the time from Lagrange to Cauchy inclusive; that at the beginning of this period group theory was a means to an end and not an end in itself. Lagrange and Ruffini thought of substitution groups only in so far as they led to practical results in the theory of equations. Galois, while broadening and deepening the application to the theory of equations may be considered as taking the initial step toward abstract group theory. In Cauchy while a group is still spoken of as the substitutions that leave a given function invariant, and the order of a group is still thought of as the number of equal values which the function can assume when the variables are permuted in every possible way, nevertheless quite as often a group is a system of conjugate substitutions and its relation to any function is entirely ignored.

In Cauchy's work it is to be noted that use is made of all the concepts originated by the earlier writers in substitution theory except those of Galois, a number of which would have proved powerful instruments in his hands, notably the idea of the invariant subgroup of which he makes no explicit use.

Because of the important theorems Cauchy proved, because of the break which he made in separating the theory of substitutions from the theory of equations and because of the importance that he attached to the theory itself, he deserves the credit as the founder of group theory.

HISTORY OF THE EXPONENETIAL AND LOGARITHMIC CONCEPTS.

By FLORIAN CAJORI, Colorado College.

V. Generalizations and Refinements Effected During the Nineteenth Century.

GRAPHIC REPRESENTATION.

The time of Wessel and Argand has been chosen as the beginning of a new epoch in our history, not because Wessel and Argand made any noteworthy advance in exponential and logarithmic theory, but because the graphic repre-

---

[1] See G. A. Miller in *Bibliotheca Mathematica* (1910), series 3, vol. 10, p. 321.